Ciber IA y Darktrace Cloud

Asegurando nuevos modelos de computación, aplicaciones, usuarios y dispositivos

Índice

Resumen ejecutivo

La rápida adopción de servicios en la nube y de SaaS, ha transformado la infraestructura digital y ha por completo reconfigurado el reto que plantea defender empresas contra ataques avanzados.

Impulsado inicialmente por la necesidad de reducir costes y aumentar la eficiencia, la transición a la nube sirve ahora como una vía esencial para proyectos de transformación digital – desde la aplicación de análisis avanzados a grandes conjuntos de datos, hasta el Edge Computing y dispositivos inherentes en todo, desde ciudades inteligentes a automóviles conectados. Sin embargo, desde la perspectiva de la seguridad, estos nuevos modelos de computación han ampliado la superficie de ataque a un ritmo alarmante, ya que introducen nuevos vectores de amenazas a través de una red corporativa cada vez más dispersa.

Esta tendencia presenta un reto especial para los equipos de seguridad ya agotados, ya que ahora deben hacer frente a un entorno con una visibilidad y control limitados, y en el que las herramientas de seguridad locales que ya conocen a menudo no son aplicables. Además, la facilidad con la que los programadores pueden lanzar una instancia en la nube y eludir al equipo de TI o de seguridad, puede exponer la empresa a un riesgo considerable, exigiendo un nuevo enfoque DevSecOps, algo que puede resultar inusual para los equipos que han crecido sobre la base del modelo 'on-premise' tradicional.

De manera más general, los retos de seguridad que plantea la nube se rigen en gran medida por un modelo de responsabilidad compartida, que delimita las respectivas áreas de la nube, cuya gestión y seguridad se espera que sea responsabilidad de proveedores y clientes. Mientras que la parte del modelo de responsabilidad compartida del cliente varía através de IaaS y SaaS, la idea central general del modelo ilustra claramente que la externalización de determinados procesos de TI en la nube, no equivale a la externalización completa de su función de seguridad.

La mayoría de las organizaciones reconoce esta realidad aunque pocas están satisfechas, si es que alguna lo está, con las soluciones de seguridad específicas de la nube disponibles en el mercado, tampoco pueden hacer que sus equipos adopten inmediatamente un enfoque DevSecOps como alternativa. Aunque muchos proveedores de SaaS e IaaS ofrecen controles nativos de seguridad para ayudar a los clientes a asegurar su propia parte del modelo de responsabilidad compartida, estos controles a menudo están limitados en su alcance y tienden a ser útiles para el cumplimiento, en lugar de servir de ciberdefensa proactiva y en tiempo real. Incluso en este alcance limitado, los controles nativos de seguridad solo pueden ser eficientes si se han implementado adecuadamente por el cliente de la nube.

Para complementar los controles nativos, también pueden resultar útiles soluciones de terceros tales como los agentes de seguridad de acceso a la nube (CASB, por sus siglas en inglés) y las plataformas de protección de carga de trabajo en la nube (CWPP, por sus siglas en inglés) para la aplicación de políticas y para proporcionar visibilidad en toda la nube, aunque estos se esfuerzan en detectar amenazas sutiles y comportamientos anómalos no capturados mediante reglas o políticas predefinidas. A medida que las amenazas se desarrollan y se vuelven más sofisticadas, las organizaciones requieren un enfoque fundamentalmente nuevo para proteger los entornos de la nube contra ataques avanzados, antes de que tengan tiempo de desarrollarse y provocar una crisis.

Más allá de estos controles nativos y de terceros, ¿qué situaciones se necesitan considerar para la seguridad en la nube? Algunos casos de uso adicionales incluyen:

- Lanzamiento de una instancia eludiendo los equipos de TI y seguridad
- Datos de producción que se trasladan a sistemas de prueba menos seguros
- Tráfico lateral en la nube
- Usuarios de Office 365 y Salesforce trasladando datos fuera de la nube
- Dispositivos 'edge' que utilizan la nube como vía
- Cambios sutiles e inusuales en el comportamiento de los usuarios
- Ataques a la velocidad de las máquinas que requieren una acción inmediata
- Correlación y análisis contextual para detectar anomalías
- Neutralización de correos electrónicos maliciosos en Office 365, especialmente de remitentes de confianza a lo largo de la cadena de suministro

> Darktrace Cloud representa una nueva frontera en la ciberdefensa basada en IA. Nuestro equipo ahora cuenta con cobertura completa en tiempo real a través de nuestras aplicaciones de SaaS, contenedores de nube y sensores distribuidos por toda la ciudad.
>
> **Ciudad de Las Vegas**

Basada en aprendizaje de máquina y algoritmos de IA, la tecnología de ciber IA de Darktrace llega más allá de la seguridad que proporcionan los controles nativos y las herramientas de terceros. Utilizando software y sensores, Darktrace Cloud cubre todos los casos de uso indicados anteriormente mediante análisis robusto de tráfico y el flujo de data a través de los entornos de nube y SaaS. La IA de Darktrace aprende el 'patrón de vida' normal de cada usuario, dispositivo y contenedor –sin depender de presuposiciones ni ingreso manual de datos.

Esta evolución en la comprensión de lo 'normal', permite a la plataforma detectar y responder de manera autónoma a ataques externos y amenazas internas en tiempo real, ademas de proporcionar visibilidad completa de todo el negocio digital en una sola pantalla. Este informe técnico examina las vulnerabilidades de seguridad que cubre la plataforma de Darktrace usando IA y aprendizaje de máquina. Mediante el aprendizaje de todo el alcance del 'patrón de vida' cambiante de su organización, la IA de Darktrace resulta especialmente adecuada para detectar y neutralizar desviaciones sutiles indicativas de una amenaza en la nube, en colaboración con su siempre cambiante patrimonio digital.

Vectores de amenazas en la nube

El modelo de responsabilidad compartida en la nube delimita las respectivas funciones de seguridad de los proveedores de servicios en la nube (CSP, por sus siglas en inglés) y de los clientes a través de los principales modelos de servicio: Infraestructura como servicio (IaaS, por sus siglas en inglés) para sistemas y almacenamiento y software como servicio (SaaS, por sus siglas en inglés) para aplicaciones empresariales .

Con la IaaS, el CSP asume por completo la responsabilidad de proteger los componentes de la infraestructura –incluyendo servidores, redes, máquinas virtuales y contenedores–, mientras que se espera que el cliente gestione el sistema operativo invitado, cualquier software de aplicación y la configuración de los controles nativos de seguridad. Con SaaS, el CSP es responsable de la infraestructura y las aplicaciones, mientras que el cliente debe asegurarse de que la actividad del usuario y de la red está correctamente gestionada y protegida. Esto conduce a un conjunto específico de vectores de amenazas a los que el cliente de la nube debe ser capaz de hacer frente, aunque la mayoría de los controles nativos de seguridad y ofertas de terceros están mal equipados para detectarlos en etapas tempranas.

Gartner prevé que para el año 2022, al menos el 95% de los fallos de seguridad en la nube van a suceder en la parte del cliente del modelo de responsabilidad compartida. Esta es una cifra asombrosa, pero al desentrañar los principales vectores de amenazas que pueden provocar estos fallos, podemos comprender mejor qué puede hacer el cliente de la nube para mitigar estos riesgos de forma eficiente.

Amenazas internas

La mayor parte de la industria reconoce que los líderes de CSP y proveedores de SaaS son altamente resistentes a las brechas de seguridad, al menos en su parte del modelo de responsabilidad compartida. Sin embargo, los retos particulares introducidos por la nube –desde la falta de visibilidad y control a la nueva manera de pensar, aún desconocida, requerida por la agilidad y velocidad de la infraestructura digital–, han magnificado los riesgos tradicionales que caen en la parte de responsabilidad del cliente.

En particular, las amenazas internas representan un peligroso vector de ataque que siempre ha planteado un riesgo, pero ahora ha adquirido una nueva dimensión y agilidad a través de la nube. Estos tipos de ataques se originan dentro de la organización –ya sea por parte de empleados descontentos, descuidados o comprometidos o de asesores de la nube y otros socios comerciales que abusan de su acceso a los sistemas internos.

En particular, los intrusos maliciosos tienen la ventaja de estar familiarizados con los sistemas que manipulan y pueden dedicar tiempo a preparar y perpetrar el ataque. Mediante la filtración o manipulación lenta de datos durante días y semanas, estos actores se encuentran en una posición única para comprometer entornos de nube completos y eludir las herramientas de seguridad basadas en reglas diseñadas para monitorear actividad anormal, hasta el punto de que estas han sido implementadas en todo.

Casos famosos de amenazas internas –desde las filtraciones de Edward Snowden en 2013 al sabotaje que sufrió Tesla en 2018 por parte de un intruso– han provocado grandes repercusiones en la industria de la seguridad de TI y más allá. El hecho de que, supuestamente, la mayoría de las redes seguras podrían ser vulneradas por aquellos con suficiente motivación y conocimiento técnico, ha enviado una clara señal a los profesionales de la seguridad de que la amenaza puede ya estar dentro. Con la llegada de la nube, los equipos de seguridad se enfrentan ahora a un punto ciego crítico en un área sumamente sensible de la infraestructura, donde los intrusos pueden a menudo operar sin despertar sospechas.

Credenciales comprometidas

Por motivos similares, el riesgo de que un atacante externo utilice credenciales legítimas para obtener acceso, también se ha convertido en un riesgo crítico para organizaciones con poca o ninguna visibilidad en la nube. Utilizando el conjunto correcto de credenciales y eludiendo los controles de seguridad tradicionales, estas amenazas tienen el potencial de poner en peligro todos los activos críticos de la organización, especialmente a medida que los empleados siguen reutilizando contraseñas en sus cuentas personales y profesionales.

En la mayoría de los casos, las credenciales de inicio de sesión del empleado se recaudan a través de filtraciones de datos, exposiciones o campañas de phishing y se venden al mejor postor en la dark web. Una vez adquiridas, las credenciales se puede utilizar para moverse lateralmente dentro de la nube y acceder a sistemas y datos esenciales. Las misiones de ataque varían desde la filtración o manipulación de datos,al espionaje corporativo.

Con la IaaS en particular, las credenciales de usuario de los administradores del sistema se consideran a menudo las llaves del reino de la nube, ofreciendo a los atacantes acceso a datos confidenciales en entornos de producción y prueba, e incluso a la gestión de la propia infraestructura de la nube. Más allá de hurtar o alterar datos críticos, los ciberdelincuentes pueden utilizar las credenciales de los administradores del sistema para aprovechar la potencia de computación de la nube para sus propios propósitos infames, lanzando instancias de la nube para poner en marcha grandes operaciones de criptominería o ataques distribuidos de denegación de servicio. Para la empresas que están basadas únicamente en la nube, esta amenaza en particular supone un riesgo existencial.

Errores de configuración

Más allá de los ciberataques directos, uno de los vectores de amenazas más comunes en la nube sigue siendo los errores de configuración en entorno de IaaS. Mientras que los errores humanos son imposibles de evitar por completo, los errores de configuración son a menudo una consecuencia natural de la agilidad de implementación y la rápida instanciación de contenedores de prueba y conjuntos de datos facilitados por la nube que, a menudo, impulsa a los usuarios a moverse rápidamente a expensas de la seguridad.

En la actual infraestructura digital, los desarrolladores tienen la posibilidad de implementar una instancia de la nube en minutos, sin necesidad de consultar a los equipos de seguridad, de TI o de evaluación de la calidad. En el pasado, unos flujos de trabajo más lentos significaban que estas funciones podían permitirse trabajar en silos, pero la simplicidad y velocidad de la nube requiere aprender un enfoque DevSecOps ágil e inclusivo, lo que garantizaría idealmente que las consideraciones de seguridad influirían en una instancia de la nube determinada sin retrasar el trabajo del desarrollador.

No obstante, no todas las organizaciones están equipadas para adoptar rápidamente una mentalidad radicalmente nueva y esta agitada transición ha ofrecido a menudo como resultado errores críticos de configuración que dejan a la empresa expuesta a los ataques. En muchos casos, estos errores de configuración ocurren en un contexto de implementaciones de la nube de 'mascotas' y 'ganado', donde la 'mascota' representa a los entornos de producción bien protegidos y autorizados y el 'ganado' representa a los entornos de prueba desechables y atípicos que a menudo se crean sin pensar en los problemas de seguridad. Los errores de configuración resultantes pueden variar desde olvidarse de implementar controles nativos de seguridad a configurar entornos de prueba orientados al público, cuando no debería ser así e incluso olvidarse de que el entorno estaba destinado a desecharse en su totalidad. En este último caso, los desarrolladores podrían incluso dejar datos o credenciales reales a la vista de cualquiera, pudiendo ser recogidos por atacantes mediante exploraciones rutinarias para rentabilizarlos en la dark web.

> "Los errores de configuración de las plataformas en la nube constituyen la principal amenaza para la seguridad de la nube."
>
> **Crowd Research Partners**

Unsecured APIs

Las API no seguras se han convertido en uno de los errores de configuración en la nube más impactantes, los cuales incluyen la lista de los 10 riesgos más críticos en Aplicaciones Web de OWASP de 2017. La API de una aplicación es, en última instancia, la interfaz para los datos back-end, por lo que cualquiera vulnerabilidad en la gestión de la respuesta a errores, se convertiría en un objetivo natural atractivo para ciberdelicuentes con una amplia gama de motivaciones. Al igual que ocurre con otros errores de configuración, los desarrolladores que trabajan a la velocidad de la infraestructura digital a menudo no trabajan mano a mano con la seguridad y, a veces, pueden fallar en proteger lo suficiente las API frente a posibles abusos –desde aplicaciones de 'spoofing' a la codificación de la API para responder erróneamente a atacantes con datos altamente confidenciales.

Edge Computing

En un gran número de áreas, la potencia de computación mejorada que proporciona la nube, ha construido un trampolín para el desarrollo de tecnologías nuevas e innovadoras.

En particular, el Edge Computing destaca como una de las más notables ramificaciones de la nube, incluso cuando representa un alejamiento radical del procesamiento de datos en nodos centrales –acercando la lógica de la computación a las fuentes físicas de datos para reducir la latencia y aumentar el ancho de banda.

Por ello, los análisis de datos están llegando cada vez más hasta el límite, donde sensores distribuidos, dispositivos del IoT e incluso aplicaciones, pueden tomar decisiones rápidas en tiempo real, teniendo solo que enviar los datos procesados de vuelta a la nube cuando estén listos para ser almacenados o agregados de otro modo.

Mientras que la nube está siendo posiblemente relegada a un segundo plano en este caso de uso, la explosión de el Edge Computing y de los dispositivos en plantas de fabricación, ciudades inteligentes y plataformas petrolíferas, sigue ampliando la superficie de ataque a través de las cuales, las amenazas pueden encontrar, finalmente, su camino de vuelta a la nube central.

Limitaciones de herramientas de seguridad nativas y de terceros

En este contexto de evolución de las amenazas, los CSP y otros proveedores han desarrollado una gama de herramientas de seguridad para ayudar a defender a la parte del cliente del modelo de responsabilidad compartida. Mientras que estas soluciones pueden proporcionar alguna medida de protección, generalmente están equipadas deficientemente para defenderse contra amenazas avanzadas que se ejecutan desde la nube.

Controles nativos de seguridad del CSP

Además de asegurar su propia parte del modelo de responsabilidad, la mayoría de proveedores de la nube ofrecen soluciones nativas para ayudar a los clientes a implementar medidas básicas de ciberhigiene en la nube. Estas pueden incluir desde firewalls, autenticación de dos factores y herramientas de IAM, hasta monitorización de registros e integraciones de conocimientos sobre amenazas.

Aunque estos controles nativos constituyen un buen comienzo y pueden contribuir positivamente a la eficiencia de la estrategia de defensa general de su organización, a menudo no son suficientes en la práctica. A medida que las organizaciones continúan adoptando servicios en la nube de múltiples proveedores, no es posible confiar en que los controles nativos proporcionen una cobertura completa, ya que con frecuencia se diseñan exclusivamente para el entorno de nube del proveedor específico.

La mayoría de las empresas que migran sus cargas de trabajo a la nube, utilizan múltiples proveedores de IaaS, mientras que un estudio realizado a principios de 2018 encontró que el número promedio de aplicaciones en la nube, utilizadas en el entorno empresarial, ha aumentado hasta casi 2.000. Ahora que las implementaciones 'multinube' se han convertido en la norma, los enfoques descontextualizados hacia la seguridad de la nube han quedado desfasados y aumentan la demanda por soluciones agnósticas de proveedores que incluyen toda la gama de entornos de nube y SaaS. También vale la pena destacar que todos los controles nativos de seguridad deben ser implementados correctamente por el cliente, quien posiblemente no esté familiarizado con la configuración de estas herramientas en la nube.

> "Con nuevas amenazas a enfrentar diariamente, las herramientas tradicionales diseñadas para detectar amenazas conocidas ya no son suficientes."
>
> **Inphi**

Sin embargo, si se han implementado y configurado correctamente en una empresa de una sola nube, la mayoría de los controles nativos de seguridad también tienden a ser más útiles para el cumplimiento normativo que para la ciberseguridad. Mientras que los registros que recopilan pueden entregarse a auditores para demostrar algún nivel de visibilidad en la nube, esta vista es a menudo retrospectiva y es improbable que capture las amenazas más graves. A medida que los ciberdelincuentes siguen explotando los puntos flacos de la nube, la monitorización de registros apenas será suficiente para capturar a los atacantes furtivos y silenciosos que acechan bajo la superficie.

Herramientas específicas de la nube de terceros

Otros proveedores también han comenzado a desarrollar soluciones de seguridad específicas para la nube tales como los agentes de seguridad de acceso a la nube (CASB, por sus siglas en inglés) y las plataformas de protección de carga de trabajo en la nube (CWPP, por sus siglas en inglés) para llenar los vacíos dejados por los controles nativos. Los CASB se han diseñado esencialmente para proteger aplicaciones de SaaS , ofreciendo características de visibilidad en la nube, DLP y cumplimiento. El objetivo de las CWPP es ofrecer cobertura a entornos de IaaS híbridos, ofreciendo controles de aplicación basados en listas blancas, así como funciones de visibilidad en la nube y segmentación de la red en contenedores y cargas de trabajo.

En términos generales, los CASB y las CWPP se especializan en controles preventivos, cumplimiento y visibilidad en el marco de sus respectivos casos de uso. Aunque estas funciones desempeñan su cometido, a menudo no logran atrapar ataques sutiles ni dirigidos. La mayoría de los proveedores de esta área han reconocido este hecho y algunos han intentado implementar la funciones rudimentarias de detección de anomalías como complemento, estableciendo un punto de referencia estático y predefiniendo comportamientos inofensivos y maliciosos. Sin embargo, no puede esperarse que este enfoque tradicional proporcione suficiente protección contra ataques avanzados, incluso a pesar de que estos mercados siguen madurando.

Darktrace Cloud

La tecnología de ciberinteligencia artificial de Darktrace aporta un enfoque único para la ciberdefensa en tiempo real en la nube. Desarrollado sobre la base del aprendizaje automático no supervisado y la IA, Darktrace Cloud analiza los flujos de datos en y a través de las aplicaciones de SaaS y cargas de trabajo de la nube, aprendiendo el 'patrón de vida' normal de cada usuario, dispositivo y contenedor. Mediante la correlación de desviaciones sutiles del comportamiento en tiempo real, Darktrace Cloud puede detectar y detener una gama completa de ciberamenazas en la nube, desde intrusos maliciosos y ataques externos, hasta errores de configuración críticos que pueden comprometer la infraestructura y ejercer un alto impacto a través del patrimonio digital.

El poder de la tecnología de Darktrace reside en un enfoque de autoaprendizaje que no depende, con antelación, de comportamientos 'inofensivos' o 'maliciosos' predefinidos. En su lugar, Darktrace Cloud crea modelos de comportamientos normales de usuarios, contenedores y dispositivos en relación a su pasado, sus grupos de compañeros y el resto de la organización, revisando continuamente sus cálculos a la luz de nuevas pruebas y correlacionando indicadores débiles para establecer una medida que evoluciona de la probabilidad de amenazas.

El enfoque de Darktrace resulta esencial en esta nueva era de ciberamenazas basadas en la nube, donde los intrusos con acceso privilegiado y actores externos con credenciales de administrador pueden atravesar toda la infraestructura de la nube sin activar alarmas. No se puede (ni debería) esperarse que el proveedor de la nube proteja la nube contra conexiones de confianza, mientras que las herramientas de terceros con capacidad para detectar anomalías solo pueden hacerlo de un modo básico y sencillo. Sobre la base de períodos de aprendizaje fijo y nociones predefinidas de comportamientos 'inofensivos' y 'maliciosos', estas herramientas solo pueden detectar las amenazas más evidentes. Por el contrario, el aprendizaje de máquina sin supervisión y la IA de Darktrace pueden ir más allá de lo que los seres humanos ya conocen o pueden imaginar, y detectar desviaciones sutiles que pueden indicar el desarrollo de una amenaza.

En lugar de basarse en reglas y políticas predefinidas, Darktrace Cloud adopta la incertidumbre inherente en el actual complejo entorno digital. Todas las desviaciones significativas son detectadas y correlacionadas, lo que ofrece como resultado la detección de amenazas reales sin producir avalanchas de falsos positivos.

> "Darktrace Cloud funciona perfectamente para AWS. Es sencillo, fácil de usar y nos hace sentir mucho más cómodos lanzando nuestra infraestructura en la nube."
>
> **Innovating Capital**

Darktrace Cloud para IaaS y SaaS

Darktrace Cloud puede integrarse fácilmente con su diverso patrimonio digital, incluyendo los entornos de IaaS como AWS y Azure, y aplicaciones de SaaS como Salesforce, Box, G Suite, Dropbox y Office 365.

box
salesforce
Microsoft Azure
aws
Office 365
Dropbox
rackspace
the open cloud company
Google Cloud Platform
G Suite
EGNYTE

Darktrace Antigena: Respuesta autónoma en la nube

La IA de Darktrace no solo detecta sino que además responde de forma autónoma a las amenazas cibernéticas en curso en la nube. Darktrace Antigena, el modulo de respuesta autónoma de la plataforma, utiliza la inteligencia artificial para adoptar acciones específicas y dirigidas en respuesta a ciberamenazas de alta confianza, deteniendo su propagación en tiempo real y ofreciendo al equipo de seguridad el tiempo necesario para ponerse al día.

Los distintos tipos de acciones que puede emprender Darktrace Antigena varían dependiendo del tipo específico de entorno en la nube o aplicación de SaaS que se está utilizando, tal y como se ilustra en las listas de abajo, que no son exhaustivas ni definitivas a traves de todas las plataformas en la nube o SaaS .

Para neutralizar los ataques en curso en ambientes en la nube como AWS y Azure, Darktrace Antigena puede:

- Interrumpir el funcionamiento de una máquina virtual o editar sus propiedades.
- Editar los permisos de acceso a buckets S3 de AWS
- Desactivar temporalmente el acceso programático de un usuario
- Restablecer las contraseñas de usuario para desactivar el acceso de administración
- Editar los permisos de usuario
- Detener temporalmente la difusión de un documento

En aplicaciones de SaaS como Office 365, Salesforce, G-Suite y Box, Darktrace Antigena puede:

- Interrumpir las sesiones activas de un usuario
- Desactivar usuarios temporalmente
- Restringir o eliminar los ajustes para compartir archivos de ciertos archivos y carpetas
- Restringir el acceso a un usuario a ciertas partes del entorno en la nube
- Suspender a miembros de equipos y, por lo tanto, su acceso a determinados archivos compartidos (en Dropbox, por ejemplo)

Darktrace Threat Visualizer: visibilidad completa

La mayoría de las organizaciones que migran infraestructura y aplicaciones a la nube, luchan con la visibilidad de la migración y su control. Incluso los equipos de seguridad que configuran e implementan correctamente herramientas nativas y de terceros, rara vez tienen acceso a una visibilidad pormenorizada en tiempo real que les permita monitorear continuamente las investigaciones de amenazas interactivas y contextualizadas.

Para proporcionarle esta visibilidad en su infraestructura digital, la interfaz gráfica de Darktrace Threat Visualizer proporciona una única pantalla que permite la visualización e investigación en tiempo real de actividades anómalas en cargas de trabajo, aplicaciones de SaaS y en cualquier lugar de la nube. El Threat Visualizer se ha diseñado para usuarios de todos los niveles de madurez, desde expertos en seguridad forense a ejecutivos de negocios y miembros de equipos de TI menos experimentados.

Permite la consulta y exposición de una gran cantidad de información usando las funciones interactivas del Threat Visualizer, incluyendo un panel dinámico que permite a los usuarios filtrar incidentes dependiendo del nivel de gravedad y una herramienta de reproducción interactiva que permite a los usuarios reproducir incidentes y concentrarse en el contexto de cada evento en tiempo real.

> “Con Darktrace Cloud, podemos iluminar los rincones más oscuros de nuestra red.”
>
> **Addivant**

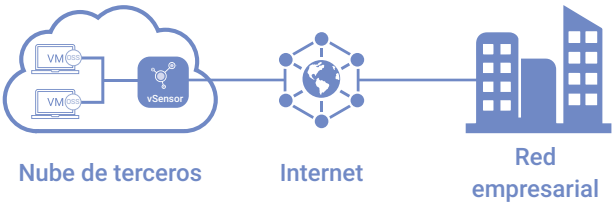
Escenarios de implementación de tecnología

Nube híbrida (IaaS)

Para implementación en la nube, perimetrales y físicas, los sensores OS basados en el host se instalan en cada extremo de la nube y se configuran para enviar copias inteligentes del tráfico de la red a un vSensor local implementado en el mismo entorno de la nube. El vSensor receptor procesa los datos y los envía de vuelta al software de Darktrace en la empresa, que correlaciona el comportamiento en todos los entornos de la nube y físicos de la organización.

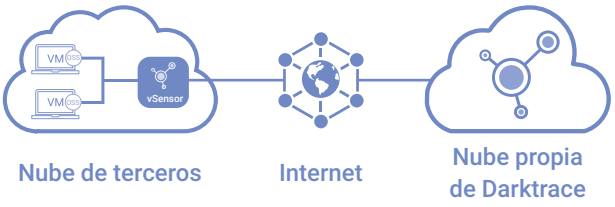
Además, los clientes de AWS y Azure pueden optar por utilizar los conectores de Darktrace para monitorizar la actividad del administrador del sistema que no puede ser percibida por el sensor OS. empresarial como, por ejemplo, inicios de sesión, cambios en archivos o transferencias de datos.

> "Cuando activamos Darktrace Cloud, fue como prender un foco en una habitación oscura"
>
> **TRJ Télécom**



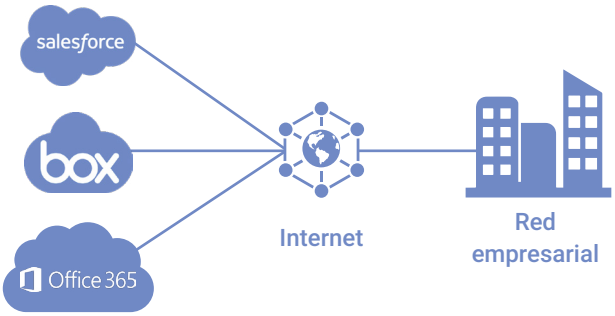
Solo nube (IaaS)

Para las organizaciones que ejecutan sus propias infraestructuras exclusivamente en la nube, Darktrace puede gestionar la implementación como un servicio dedicado, instalando vSensors y sensores OS en el entorno de nube de la organización y enviar los datos de vuelta a un instancia en la nube de Darktrace para su análisis.



SaaS

Para implementaciones de SaaS, los conectores de SaaS de Darktrace se instalan de forma remota en la red empresarial e interactúan directamente con la API de seguridad del proveedor de SaaS a través de solicitudes HTTPS . Esto permite a Darktrace procesar y monitorear las interacciones de los usuarios a los pocos minutos de su creación, independientemente de que se originen dentro de la red o desde ubicaciones remotas.



Descubrimientos de amenazas reales

Robo de datos internos de la nube

Una empresa de retail decidió reestructurar su departamento de TI. Al hacerlo , tuvieron que despedir a varios empleados. Uno de los empleados afectados –un director de TI– descargó información de contacto y números de tarjetas de crédito de la base de datos de clientes. Darktrace detectó las transferencias de datos hasta un servidor, a través del servicio de transferencia de datos regular de la empresa. El empleado intentaba probablemente vender la información para sacar un beneficio.

La base de datos se mantenía en servicio en la nube de otro proveedor con el objetivo de flexibilizar el trabajo y reducir los costes de hardware. Este modelo empresarial se basaba en gran medida en el uso de los servicios de sincronización, almacenamiento y transferencia de archivos de la nube. Sin embargo, este director de TI demostró el modo en que podían explotarse los servicios de la nube para la filtración de datos internos.

El departamento de marketing de la empresa utilizaba frecuentemente este servicio en la nube, pero resultaba altamente inusual que un director de TI enviara datos externamente a través de la nube.

Darktrace fue capaz de hacer esta distinción porque aprende continuamente la actividad normal de cada usuario y dispositivo, y compara el comportamiento entre dispositivos para identificar similitudes.

La tecnología de Darktrace detectó esta ligera desviación del 'patrón de vida' normal, permitiendo a la plataforma identificar este comportamiento sutil y amenazador, a pesar de que el servicio en la nube se utilizaba regularmente para fines legítimos.

Darktrace detectó estas anomalías en tiempo real y proporcionó a la empresa información detallada sobre la naturaleza exacta del problema. Tras ello, se revocaron las credenciales del empleado y la empresa recuperó y protegió rápidamente los datos de los clientes.

Ataque externo en el perímetro de la nube

Una organización de servicios financieros alojaba distintos servidores críticos en aplicaciones virtuales en la nube, algunos de las cuales estaban orientados al público mientras que otros no lo estaban.

Al configurar la implementación en la nube, dejaron por error un importante servidor expuesto a Internet cuando se suponía que debía estar aislado por un firewall. Esto podría haber sucedido por multitud de razones, posiblemente debido a una migración rápida y caótica o bien, porque el equipo de seguridad simplemente no estaba muy familiarizado con el firewall nativo proporcionado por su CSP.

El servidor expuesto sufrió un bombardeo continuo de ataques de terceros malintencionados que intentaban acceder a dicho dispositivo y, desde allí, acceder a la nube y posiblemente de vuelta al centro de su red física. Lo peor de todo es que el cliente no se había dado cuenta de esto porque no tenían visibilidad de lo que sucedía en su nube.

Sin embargo, tras una rápida instalación, Darktrace detectó rápidamente que el dispositivo estaba recibiendo una cantidad inusual de intentos de conexiones entrantes desde una amplia gama de fuentes externas.

Darktrace identificó el patrón de ataque y alertó al cliente del riesgo en curso. De este modo, pudieron desactivar esta brecha en su seguridad y proteger el perímetro de su nube antes de convertirse en víctima de un ataque de denegación de servicio más serio o de que este ataque hubiera logrado acceder y filtrar datos desde allí.

Al aportarles esta visibilidad, para Darktrace fue muy sencillo ayudarles rápidamente para entender lo que estaba sucediendo en la nube. Este problema no fue complicado de solucionar pero sin disponer de ningún tipo de visibilidad, nunca habrían podido detectar como se desarrollaba.

Conclusión

A medida que las organizaciones confían cada vez más en los servicios en la nube y aplicaciones de SaaS para racionalizar sus prácticas empresariales, el paradigma familiar del perímetro de la red se ha disuelto, dejando en su estela un patrimonio digital poroso y siempre cambiante.

Mientras que las ventajas de la computación en la nube garantizarán la continuación de las migraciones a buen ritmo, los retos de seguridad únicos que plantea la nube no solo exigirán una mentalidad más ágil , sino también tecnologías con capacidad de autoaprendizaje que puedan moverse a la velocidad de las implementaciones en la nube y detectar desviaciones sutiles indicativas de una amenaza, ofreciendo al mismo tiempo una visibilidad completa y en tiempo real de toda la infraestructura digital.

El liderazgo mundial de Darktrace en el campo de la inteligencia artificial para la ciberseguridad convierte a esta solución en la más eficaz ya que ha demostrado ser capaz de detectar amenazas sin precedentes e incidentes cibernéticos anómalos. Independientemente de que se enfrente a una amenaza interna, un atacante centrado en datos confidenciales en contenedores de prueba o un error de configuración significativo que podría aprovecharse en el futuro, la plataforma de ciberinteligencia artificial de Darktrace ayuda a eliminar puntos ciegos y proteger sus datos independientemente del lugar donde residan.

> “Darktrace detecta y responde a las amenazas que pasan desapercibidas para otras herramientas.”
>
> **IDC**

Más información

darktrace.com | @darktrace | LinkedIn